P518081.PDF [Page: 3 of 27]

DEFENCE R&D DÉFENSE

Managing Identity and Access in a Classified Defence Environment

31 October 2001

Alan Magar
Magar Security Architecture Inc.

Defence R&D Canada

CONTRACT REPORT
DREO CR 2001-081
October 2001

National Defence Défense nationale

Canada

P518081.PDF [Page: 4 of 27]

105-03215/

Executive Summary

The classified defence environment is an extremely challenging environment where the rigorous protection of information assets has necessitated the adoption of a predominantly network-based information security model operating in System High Mode. Two innovative technologies, Public Key Infrastructure and Privilege Management Infrastructure, provide the underlying infrastructure with which to manage identity and access throughout an organization. This paper will examine how these two technologies can be enhanced in order to transition the classified defence environment to a content-based information security model capable of providing Multi-Caveat Separation and eventually supporting Multi-Level Security mode.

P515081.PDF [Page: 5 of 27]

Table of Contents

1.0 INTRODUCTION 1

2.0 DEFENCE ENVIRONMENT 2

2.1 System High Mode 3
2.2 Multi-Caveat Separation 4
2.3 Multi-Level Security Mode 4
2.4 Information Assurance 4

3.0 MANAGING IDENTITY 5

3.1 Something You Know 7
3.2 Something You Have 7
3.3 Something You Are 9
3.4 Registration 9

4.0 MANAGING ACCESS 10

4.1 Why not Public Key Certificates? 10
4.2 Why not Attribute Certificates? 11
4.3 Standard PMI 12

5.0 ENHANCED PMI PROPOSAL 13

5.1 Access Rights Management 14
5.2 Electronic Sensitivity Labeling 15
5.3 Policy-Enforced Access Control 16
5.4 PKI Integration 17

6.0 CONCLUSIONS 18

7.0 REFERENCES 19

1.0 Introduction

Until the late seventies information security was almost exclusively the domain of the military. It was used to protect one's own information assets while at the same time exploiting those of the enemy. Before long private companies began to see the benefit in protecting their intellectual property and other information resources from competitors, hackers and even malicious employees. Initially this led to a small number of information security companies leveraging the work done previously in this area by the military. The end result is a booming information security industry employing thousands and spending millions of dollars annually on research and development.

Defence departments came under considerable budgetary constraints with the end of the Cold War. In-house software, with its prohibitive development and maintenance costs, was one of the first casualties. As a result defence departments have become increasingly reliant on Commercial-Off-The-Shelf (COTS) products. Unfortunately, these COTS products are not designed specifically for the military. Rather, they are developed according to the requirements of their primary market, Fortune 500 companies.

The same is true with regard to managing identity and access. Two innovative products have been developed, primarily in the private sector, for the private sector. They are Public Key Infrastructure (PKI) and Privilege Management Infrastructure (PMI). Defence departments are currently using PKI quite extensively and are examining the use of PMI to protect their information assets. This paper addresses managing identity and access in a classified defence environment. The classified environment is selected over the more general environment for the following three reasons:

- The classified defence environment is, by far, the most challenging defence environment. It contains the most sensitive material and consequently has the most stringent requirements for information protection.
- Any solutions for the classified defence environment can be adapted not only to an unclassified environment, but also to other environments as well. The opposite is generally not true.
- Similar initiatives are currently being undertaken in the federal government that encompass the unclassified defence environment to varying degrees. The Government of Canada Public Key Infrastructure (GoC PKI) and the Government of Canada Electronic Authorization project (see Note below) are two such initiatives.

Specifically, after reviewing the unique requirements of the classified defence environment, this paper examines how PKI can be adapted to this particular environment then proposes an enhanced PMI capable of managing access in this environment.

Note – Government of Canada Electronic Authorization Project

The Government of Canada Electronic Authorization project [Ele01] is a fairly recent initiative by the federal government to provide its departments with a PMI based upon COTS authorization products. While it is anticipated that this initiative will meet the majority of federal departments' internal business and external Electronic Service Delivery (ESD) requirements, those involved in the project are fully cognizant of the existence of departments with unique requirements outside of the scope of the project. The classified defence environment is most certainly beyond the scope of this particular project.

P518081.PDF [Page: 7 of 27]

2.0 Defence Environment

The defence environment addressed in this paper is based primarily on the Canadian Integrated Information Environment (IIE), and to a lesser extent the U S Defense Information Infrastructure (DII), but should be applicable to most allied defence environments In considering the defence environment, it is important to note the following similarities to, and the differences from, the private sector

The defence environment shares the following characteristics with the private sector

- **Reliance on Information Resources** – Defence departments, perhaps even more so than private companies, rely heavily on the timely availability of accurate information resources to conduct their operations

- **Disparate Information Systems** – The defence environment, like the information technology environment of many large corporations, includes a myriad of disparate Communications and Information Systems (CISs) This diverse CIS environment complicates all aspects of information security

- **Networked Environment** – Most information systems in a private company are networked together, to the Internet, to partners and suppliers, etc to facilitate the exchange of information in order to conduct business Somewhat surprisingly, the same is true in a classified defence environment While most classified networks will generally never be connected to public networks, such as the Internet, they are interconnected with other national classified networks and allied classified networks in order to conduct multi-national operations and exercises This creates a shared-risk environment where the compromise of a single trusted information system can potentially compromise the entire network

- **High Turnover of Personnel** – Private companies are struggling to retain skilled personnel in the new economy Stiff competition in the form of higher salaries, attractive benefits and stock options are regularly siphoning away talented employees, resulting in high employee turnover and increasing reliance on out-sourcing The situation is as bad or worse in the defence environment Defence departments are unable to compete with the salaries and perks offered by private companies Furthermore, as a result of regular postings, military personnel change positions at least once every three years This is exacerbated by deployments for peacekeeping missions and other multi-national operations

Where the defence environment differs significantly from the private sector is in the area of security In a private organization there is a definite hierarchy amongst employees, with private folders and e-mail groups established to control the dissemination of company information This process is in place to restrict the distribution of sensitive company information to a limited group of high-level individuals and to prevent the average employee from being barraged with information that is irrelevant to his job In a defence environment the control of information is much more strictly regulated Information is assigned a security classification (see Note below) based on its sensitivity and the potential ramifications if its security were to be compromised In principal, only personnel with the appropriate security clearance and a need-to-know should be granted access to the information

There are two reasons for these differences between the two environments In a private organization the result of a security compromise is most probably a financial loss either directly or from the loss of a competitive advantage However, in a defence environment the consequences of a security compromise are potentially much more serious since national security and possibly lives are affected Second, security classifications and clearances are extremely costly to

P518081 PDF [Page: 8 of 27]

implement and as a result do not have the same priority in the profit-oriented private sector as the publicly-funded defence environment

This section examines a number of issues that defence departments are struggling with The intention is to provide the background information necessary to understand the discussion of managing identity and access in this environment Specifically, this section will highlight the problem of System High Mode, the concept of Multi-Caveat Separation, the panacea of Multi-Level Security Mode and the necessity for Information Assurance

Note: Clearances, Classifications & Caveats

A defence environment controls access to sensitive information and resources through the use of clearances, classifications and caveats. Information is classified according to its sensitivity and the potential consequences of a security compromise Unclassified information is considered non-sensitive and in many cases may even be made publicly available. There are four classifications normally used, UNCLASSIFIED, CONFIDENTIAL, SECRET and TOP SECRET. Information other than UNCLASSIFIED is sensitive and could have national security implications if compromised. There are three distinct levels of confidential information, PROTECTED A, PROTECTED B and PROTECTED C. Confidential information usually consists of information concerning individuals (e.g. performance evaluations, medical reports, etc) or military processes that could be potentially damaging to an individual or the department if it were to be disclosed Classified information, of which there are two classifications (SECRET and TOP SECRET), is highly sensitive information that could have national security implications if it were to be compromised

Classified information can also be sub-divided into security categories or caveats [Cav01] A caveat is an additional restriction to an existing security classification. For example SECRET CANUS material is automatically restricted to Canadian and US personnel with a Secret level clearance The caveat CANUS is an acronym for Canadian and United States. Likewise, TOP SECRET CEO material is automatically restricted to Canadian personnel with a TOP SECRET clearance The caveat CEO is an acronym for Canadian Eyes Only. The majority of caveats consist of a nationality restriction (CEO, CANUS, CANUK, AUSCANZUKUS+, etc) but others restrict access based on distribution (e.g NATO, K4, S4, etc) or the sensitivity of a topic (e g Crypto Security, Warning Notice Intelligence Sources and Methods Involved, Atomal, etc)

Defence personnel are subject to periodic background checks in order to determine an individual's suitability for a security clearance. A security clearance enables an individual to view information of the same or a lower level providing that they have a need-to-know. For example, Canadian military personnel with TOP SECRET clearance will be able to view material classified TOP SECRET CEO provided they have a requirement to view such information They would likely be unable to view material classified Secret CANUS if it was outside of the scope of their work

2.1 System High Mode

All military personnel with access to a classified network must possess a security clearance for the highest classification level of the information processed in the network However, personnel with the appropriate level of security clearance must also have a requirement or a need-to-know to view a particular item of classified information This mode of operation, which is called System High Mode, is used throughout both the Canadian IIE and the US DII The problem with System High Mode is that it necessitates building a distinct network for each level of classification This is compounded by the additional networks required for multi-national operations

P518081.PDF [Page: 9 of 27]

This raises an interesting point. If the inherent security controls provided by the applications and operating systems used in the classified defence environment are insufficient to separate multiple security classifications, or to enforce caveat separation, then they are likely insufficient to prevent those individuals without a need-to-know from accessing classified information. Seemingly, this situation is in violation of a basic security premise, least privilege. Least privilege is the practice of limiting user access to the systems and information necessary for them to accomplish their work objectives.

2.2 Multi-Caveat Separation

The first step in remedying the deficiencies of System High Mode is to allow multiple caveats at the same classification to be processed on the same network. In this scenario a SECRET network would be capable of processing SECRET CEO, SECRET CANUS and SECRET NATO information for example. The security controls, specifically authentication and access control, must be sufficiently robust to ensure that the respective nationalities are restricted to the appropriate information. This situation is referred to as Multi-Caveat Separation.

Multi-Caveat Separation has the additional benefit of ensuring that individuals are restricted to the information which they have a legitimate requirement to access regardless of their security clearance. As a result, the potential damages that could be caused by a rogue individual with a legitimate security clearance is limited to the information directly related to his occupation as opposed to potentially any information for which he is cleared.

The necessity for Multi-Caveat Separation is best illustrated by the Canadian Command Control Information Systems (CCIS) [Cav01]. The CCIS was until recently classified SECRET CEO. However, due to the fact that one Canadian CCIS (Maritime Command Operational Information System) has connections to US systems (CINCLANFLT in Norfolk and CINCPACFLT in Hawaii) and there is minimal protection between Canadian systems the entire classified domain was converted from SECRET CEO to SECRET CANUS. This move necessitated developing a solution for material that is SECRET CEO. Options included processing the data on a TOP SECRET CEO system, developing a dedicated SECRET CEO system, re-classifying the material SECRET CANUS or developing a multi-caveat separation capability. Given the obvious limitations of the first three solutions it goes without saying that the multi-caveat approach is the preferred solution.

2.3 Multi-level Security Mode

While Multi-Caveat Separation is highly desirable, it is the ability to process classified information in Multi-Level Security (MLS) mode, rather than in System High Mode, that is the ultimate goal of information security in a defence environment. A network operating in MLS mode must be sufficiently secure so as to restrict access to classified information to personnel with the appropriate security clearance and a need-to-know. Multi-Level Security mode would enable all classified data, regardless of its classification and respective caveats, to be processed on a single network. In other words, not all personnel with access to a system would need to be cleared for all of the information on that system. This would drastically reduce network infrastructure costs, improve secure information exchange and facilitate multi-national operations.

2.4 Information Assurance

Historically, defence departments have been hesitant to utilize COTS products on classified networks for fear that they will contain faulty or malicious code that could compromise their network. Furthermore, in the case of information security the majority of the expertise was

P518081.PDF [Page: 10 of 27]

concentrated in defence departmentts so there was little point in outsourcing the development of this technology However, due to the exorbitant costs inherent in developing and maintaining proprietary software, and the level of expertise now in existence in the private sector, attitudes have gradually shifted The use of COTS products in classified defence environments is not only allowed but is strongly encouraged

To mitigate the risk the US government developed security evaluation criteria for COTS products entitled Trusted Computer System Evaluation Criteria (TCSEC) or as it is more commonly referred to, the Orange book COTS products are evaluated against TCSEC by the National Computer Security Center and a rating is granted based on the product's ability to perform its stated function securely For example, C2 is the minimum security rating required by many public and private organizations which allows the processing of highly sensitive or classified information Similar security evaluation criteria were developed in both Canada (CTCPEC – Canadian Trusted Computer Product Evaluation Criteria) and Europe (ITSEC – Information Technology Security Evaluation Criteria) These multiple security evaluation criteria created a problem for product vendors Having undergone an expensive and time-consuming process to achieve accreditation under one security evaluation criteria they needed to repeat the process under a different security evaluation criteria in order to access that particular market This difficult situation was rectified in 1999 with the development of ISO standard 15408, the Common Criteria (CC) CC aligned the various security evaluation criteria so that an IT security evaluation conducted in Australia, Canada, France, Germany, New Zealand, the United Kingdom or the United States is recognized and accepted in the rest of the countries

COTS security products, including PKI and PMI products, need to be evaluated to an appropriate level in order to be considered for use in a classified defence environment, to provide Multi-Caveat Separation or in a Multi-Level Security mode capacity For example, in the Canadian CCIS [Cav01] a workstation must be certifiable to C2 level of assurance in order to be capable of providing caveat separation. The Canadian Forces Information Operations Group (CFIOG) Information Protection Center (IPC) gave approval in principle for the use of an evaluated PKI product, with a certified network operating system, to separate caveats This approval in principle was initially provided in May 1997 and confirmed in June 1999

3.0 Managing Identity

The electronic identity of an individual is represented by a username or user I D To ensure that the individual is who he claims to be, most systems require the individual to prove his identity through the use of a PIN (Personal Identification Number), a password or a pass phrase Such a system, whether an application or operating system, authenticates the user based on this information Once the user has been successfully authenticated, access to information resources is based on this authenticated identity The access controls, then, are entirely dependent on the strength of the authentication mechanism used

PINs, passwords and pass phrases are considered an extremely weak form of authentication [Cha01] in that they can be purposely shared, guessed, stolen or attacked using trojan horses, viruses, keyboard sniffers, shoulder surfing, eavesdropping and social engineering Increasing the complexity of the password can reduce the effectiveness of some of these attacks However, by increasing the complexity the user is likely to either write it down, thus compromising the system security, or forget it, thereby preventing legitimate access To complicate matters further, users are typically required to remember a password for each application or system to which they have access

Cryptography provides a solution to this problem Cryptographic credentials unique to a particular individual can be used in a challenge-response scheme to prove identity The technology known as a Public Key Infrastructure (PKI) would provide the infrastructure with which to manage these

P518081.PDF [Page: 11 of 27]

cryptographic credentials in a seamless and transparent manner While PKI solves most of the problems with respect to managing identity, it creates a few of its own The most glaring of these concerns the security of the cryptographic credentials or as it is commonly referred, private key protection

> *One of the biggest risks in any CA-based system is with your own private signing key How do you protect it? You almost certainly don't own a secure computing system with physical access controls, TEMPEST shielding, "air wall" network security and other protections, you store your private key on a conventional computer There, it's subject to attack by viruses and other malicious programs Even if your private key is safe on your computer, is your computer in a locked room, with video surveillance, so that you know no one but you ever uses it? If it's protected by a password, how hard is it to guess that password? If your key is stored on a smart card, how attack-resistant is the card^ [Most are very weak] If it is stored in a truly attack-resistant device, can an infected driving computer get the trustworthy device to sign something you didn't intend to sign?* [Ell00]

This section examines the issue of private key protection in a classified defence environment The goal is that by providing an additional layer of security for the private key, the use of PKI to manage electronic identity will become the de-facto standard in the classified defence environment, just as it is quickly becoming in the unclassified defence environment (see Note below) To this end, this section will examine three forms of private key protection (something you know, something you have and something you are) and their applicability in a classified defence environment

Note – PKI Within DND and DoD

Department of National Defence (DND)

The DND PKI program will implement a PKI for the unclassified/designated information domain and a separate PKI for the classified/mission critical domain. While both PKI implementations consist of COTS PKI products the implementations differ significantly The unclassified/designated PKI consists of seven Certification Authorities (CAs), one departmental CA (subordinate to the Government of Canada CA) and six subordinate CAs (each representing one of the six Defence Wide Area Network (DWAN) domains) The primary application being supported by the DND PKI is the Defence Electronic Messaging System (DEMS).

The overall objective of the DEMS II project is to provide a comprehensive, DND/CF wide accountable electronic mail capability, providing secure and reliable communications for management traffic for up to and including the Protected B level [DMH01] The Secure Common Electronic Mail (SCEM) component of this project will provide the necessary PKI software (key management, e-mail encryption and desktop encryption software) and a smart card to every DND e-mail user (approximately 67,000 users). Smart card readers will be installed at every CEM connected PC Full scale deployment of SCEM is scheduled to run from September 2001 to June 2002

Department of Defense (DoD)

The DoD PKI program consists of both a Medium Assurance and a High Assurance PKI The Medium Assurance PKI uses COTS products to protect information related to business processes and sensitive but unclassified (SBU) data. The High Assurance PKI uses Fortezza products (family of security products built to National Security Agency (NSA) specifications) to secure classified information resources such as command and control, and combat support information. DoD started issuing certificates on 31 July 2000 for use in two primary applications; the Defense Message System (DMS) and the Defense Travel System (DTS).

P518081.PDF [Page: 12 of 27]

The Defense Messaging System is an organizational and individual messaging service for DoD users regardless of where they are stationed throughout the world. It is capable of handling all classification levels (UNCLASSIFIED to TOP SECRET), compartments and handling instructions. It accomplishes this by offering two grades of service; medium grade and high grade. Medium grade service utilizes the DoD Medium Assurance PKI while the high grade service does likewise but with the DoD High Assurance PKI. The DMS implementation is nearly finished. By the time it has been completely deployed it will be available at 270 military installations worldwide. Release 3.0 of DMS will be deployed in 2002. It is reported to *address essential intelligence community requirements and provide automated access controls for compartments, code words and caveats* [DMS01]

The Defense Travel System [DTS01] is a paperless travel system that allows the traveler to coordinate and arrange temporary duty travel more quickly and easily than using the existing system. The system will automatically issue payments to the traveler and the government credit card company once the completed travel voucher is digitally signed by the traveler and approved, using a digital signature, by the authorizing officer. According to pilot results, DTS will reduce travel claim reimbursement time from 11.3 days to 5.8 days, eliminate 19 processing steps (from 40 to 21) and reduce processing time from 4hrs 36mins to 1hr 42mins.

3.1 Something You Know

Private keys, whether they are stored locally (e.g. on a local hard drive) or on a remote server (e.g. in a public repository to facilitate roaming), can be encrypted using a password or pass phrase to construct the encryption key. Private key protection schemes based on something you know are susceptible to many of the same attacks as traditional schemes. While a PKI provides strong certificate-based authentication, protecting the private key using a password or pass phrase introduces a vulnerability into the system. Anyone with malicious intent would attack this weak point rather than attempt to break the cryptographically strong communications themselves.

3.2 Something You Have

Many of the weaknesses inherent in password-based private key protection schemes can be mitigated through the use of hardware tokens (something you have) in conjunction with passwords (something you know). Only those tokens offering a 'tamper resistant' mobile platform on which the private key is generated, stored and which performs all cryptographic functions should be considered. An intruder wishing to gain access to a user's private key must steal the hardware token in addition to the password. This makes knowledge of the password useless without possession of the device. This adds another level of security to the private key and is consistent with the idea of defence in depth practiced by many defence departments. Furthermore, the use of a token provides a mobile platform to transport the private key securely, which enables defence personnel to access information resources from any system on the classified defence network rather than limiting them to a single workstation.

The smart card is by far the most common of these types of hardware tokens. However, not all smart cards are equal and even the better ones may not be ideally suited to the classified defence environment. Many smart cards do not perform a number of cryptographic operations including random number generation, hashing and symmetric cryptography. Not only is it extremely difficult to generate random numbers (used in cryptographic key creation) in a self-contained, sealed environment but due to the low bandwidth serial interface both bulk hashing and symmetric cryptography are extremely slow. Furthermore, a number of theoretical attacks on smart cards have been devised (protocol, micro probing, side-channel and fault analysis attacks).

P518081.PDF [Page: 13 of 27]

While many of these have been found to be impractical, a number have proven successful when undertaken by a determined, well-equipped attacker

A better, and significantly more expensive, option for this environment would be a FIPS 140-1 Level 2 or higher validated PC Token (sometimes referred to as a PCMCIA Token). This type of token has most of the advantages of a smart card in addition to a faster processor capable of performing all of the cryptographic operations required. Rather than requiring a smart card reader, a PC Token requires a Type II PCMCIA reader that comes standard with nearly all laptop computers and some desktop computers

Note - Identity Cards Within DND and DoD

Department of National Defence (DND)

DND is currently deploying 80,000 smart card systems throughout the department in order to provide enhanced security for access to corporate networks and for securing intra-department communications. The smart cards, which are FIPS 140-1 validated, will be used to store a person's digital identity. This will provide an additional layer of authentication, as well as mobility, when accessing sensitive but unclassified defence information. As mentioned previously, they will be deployed as part of the Secure Common Electronic Mail component of the Defence Electronic Messaging System. Full scale deployment will take place from September 2001 through June 2002

Department of Defense (DoD)

The Common Access Card (CAC) is a smart card featuring a magnetic strip, two bar codes, and a photograph. It will serve as the standard means of identification for active duty military personnel, selected reserve forces, civilian employees and eligible contractors. In addition to replacing the existing DoD identification card, it will be the principal card used to enable physical access to buildings and controlled spaces, to enable computer network and system access and the primary platform for the PKI digital identity. Eventually, all DoD systems will be equipped with a smart card reader in order to allow the CAC to be used for network access

Information printed on the CAC includes first, middle, and last names, person designator code (i.e., active duty v. civilian), rank, Social Security Number (SSN), Geneva Convention Category, date of birth, organ donor information, and blood type. Furthermore, other unique information will be embedded in the chip. This data will include identification data (name, rank, SSN, electronic data interchange personal identifier (EDIPI)- a unique identification code used in DEERS), blood type, organ donor information, Public Key Infrastructure (PKI) certificates (ID, e-mail, and encryption), private authentication materials, date of birth, meal entitlement code, exchange code, commissary code, Morale, Welfare, and Recreation (MWR) code (i.e. to distinguish ability to use specific athletic facilities), end date (CAC non-medical benefits eligibility end calendar date), entitlement condition code, benefit end date, branch of service, personnel category (i.e., civilian, active duty, etc.), Government Agency Code, pay category, pay grade, three-digit service short name (i.e. NAV), and card management information (e.g., when the card expires, etc.) [Her01]

The Defense Enrollment Eligibility Reporting System/Real-time Automated Personnel Identification System (DEERS/RAPIDS) workstations will be capable of issuing CACs. There are currently over 1500 of these workstations at military installations throughout the world. The system uses fingerprint biometrics to authenticate the user and imprint the necessary information on the CAC. Deployment of 4.3 million CACs began in spring 2001 and is scheduled to be complete by the end of September 2002.

3.3 Something You Are

The weak link in any private key protection scheme is invariably passwords because they place the onus for security on the user. As any information security practitioner knows, this practice should be limited where possible. Biometrics (something you are) have long been a desirable alternative to passwords (something you know) as they cannot be forgotten, guessed, stolen or easily attacked regardless of the type used. Biometrics includes: fingerprint scanning, retinal scanning, iris scanning, hand geometry, signature verification, voice recognition, face recognition, etc. Unfortunately, the admirable qualities of biometrics have always been offset by an equivalent number of limitations [Fra01] that has impeded widespread deployment of these technologies. These limitations include the cost, intrusiveness and performance of biometrics. While some technologies are starting to gain acceptance in unclassified environments because of their significant reduction in cost and increase in performance, a classified defence environment may already be ideally suited for this technology.

In a classified defence environment the number of users with access to classified material is inversely related to the sensitivity of the classified material. As the sensitivity of the material increases the number of individuals with access to this material decreases. For this reason, and due to the fact that military budgets are not subject to the same considerations as commercial enterprises, the cost of the technology is not the limiting factor delaying the use of biometrics in a classified defence environment.

Biometric authentication methods are considered by many to be intrusive and therefore not publicly acceptable. Many consider the extraction and electronic storage of this type of physical information to be unacceptable due to its historical association with criminals and due to its intrusive nature which raises privacy concerns. However, the intrusiveness of this technology should be more acceptable to military personnel, including the majority of users in a classified defence environment. Military personnel are fully aware of the need for security and are accustomed to intrusive security measures (e.g. the process of security clearances).

Historically, biometrics performance is based on two factors: False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR is the rate at which unauthorized individuals are mistakenly accepted by the system. FRR is the rate at which valid users are mistakenly rejected by the system. A classified defence environment differs drastically from a public banking network like the ATM network. In a classified defence network it is far better to reject a few valid users than to compromise system security by accepting an invalid user. The opposite is true in an ATM network where it is far better to accept a relatively high number of invalid users than to reject even a single valid user. Banks must avoid inconveniencing their existing customers even if it does mean some sacrifice in security. The military has the luxury of being able to inconvenience a relatively small percentage of its members if it means a much higher level of overall security. If biometrics are used in conjunction with passwords, rather to replace them, convenience can be improved by adopting lower FRRs. A lower FRR is acceptable when using biometric authentication with other authentication factors because of the additional security provided by the other two factors (passwords and hardware tokens). "Defence in depth" states that the weaknesses of one safeguard should be balanced by the strengths of another. Passwords and hardware tokens are both susceptible to theft while biometrics are not.

3.4 Registration

In high-assurance PKI environments, such as a classified defence environment, the registration process will always require the user to appear in person with appropriate identification in order to enroll in the PKI. While inconvenient and time consuming it is an integral component in ensuring the overall integrity of the PKI implementation. In a classified defence environment, where hardware tokens will likely be used in conjunction with biometrics, the three registration

P518081.PDF [Page: 15 of 27]

procedures can be combined in order to distribute the hardware tokens, enroll the users for biometrics and issue their public key certificates

4.0 Managing Access

Once a user has had his identity successfully authenticated, the system must determine what information resources that user may access Traditionally, this was accomplished in each system or individual application using Access Control Lists (ACLs) The entitlements kept in an ACL tended to be quite basic, read, write, execute, etc Since ACLs are managed independently for the various systems and applications found in a large organization it is almost impossible to determine a particular user's privileges across all systems in the organization When a user leaves the organization it is a daunting task to remove their access privileges on each of these individual systems Likewise, when a new employee is hired it is a laborious task to provide them with all of the access privileges they require Consequently, the ACLs on the various systems quickly become out of date, contain dormant accounts (accounts that should have been removed) and rarely reflect the organization's security policy

This section examines a number of proposed solutions to this problem, including public key certificates and attribute certificates, that eventually lead to the concept of a Privilege Management Infrastructure Furthermore it shows why a standard PMI is unsuitable for the classified defence environment and outlines the required enhancements

4.1 Why not Public Key Certificates?

One proposed solution to this problem was to utilize public key certificates to convey privilege as well as identity information After considerable debate (some of which still continues today [Wil00]) it was decided that public key certificates were the wrong mechanism with which to convey privilege The reasons for this decision were as follows

- **Jurisdiction** – The entity responsible for issuing public-key certificates is unlikely to be the same entity responsible for controlling users' access to classified information resources Public-key certificates will be issued by a central, trusted authority which has a formal relationship with the individual Access privileges, on the other hand, are likely to be delegated throughout the organization to those familiar with the user, who are able to respond quickly to changes in their access requirements Assigning responsibility for both functions to one role or department increases the likelihood of a compromise By separating these functions malicious users are forced to collude to compromise the overall security

- **Interoperability** – Public-key certificate extensions are optional If an extension field is populated then applications capable of understanding it will use it while ones that don't will not The vast majority of applications understand how to extract authentication information from a public-key certificate but are less likely to be able to do the same with authorization information For this reason interoperability with respect to authorization is unlikely

- **Certificate Churn** – By placing access privilege information in a public-key certificate one drastically reduces the lifetime of that certificate Access control information changes much more frequently than does authentication information While authentication information will change with a change in job function, such as, a promotion or delegation of added responsibility Any change to the data in a certificate requires the old certificate to be revoked and a new certificate to be issued Frequent changes lead to the phenomena of certificate churn Not only would this increase the size of Certificate Revocation Lists (CRLs) substantially, it would also increase the administrative costs associated with revoking and reissuing public-key certificates A number of security practitioners [Wil00] have argued, with

P518081.PDF [Page: 16 of 27]

good reason, that public key certificates can be used to convey privilege in environments where the burden of proof of identity during the registration process is not so onerous. In these environments it would be relatively easy to re-issue public key certificates. This certainly doesn't apply to the classified defence environment where high assurance public key certificates would most definitely be used. The re-issuance of high assurance certificates would require the individual to appear at a given location and present the appropriate documentation as proof of identity.

Once it became clear that public key certificates were the wrong mechanism with which to convey privilege a similar certificate format, but lacking the public key, was developed for the express purpose of conveying privilege. Like a PKI however, attribute certificates require an infrastructure with which to manage the certificates throughout their lifecycle. This infrastructure is commonly referred to as a Privilege Management Infrastructure and it is for this reason that many information security practitioners equate a PMI with attribute certificates.

4.2 Why not Attribute Certificates?

Attribute certificates originated in international standards groups soon after the limitations of storing privilege information in public key certificates became apparent. The idea of the attribute certificate is to store privilege information in a certificate similar in form to a public key certificate but one that does not contain cryptographic key material. While the concept of attribute certificates was immediately embraced within standards groups, its reception elsewhere has been less enthusiastic. Attribute certificates are currently in use in a small number of information security products ranging from Web-based authorization solutions to Virtual Private Networks (VPNs). In each case they are used to convey privilege internally within the product rather than between products as one would expect from a true infrastructure product.

Other more ambitious uses of attribute certificates have also been proposed. For example, [Gra01] proposes the use of attribute certificates to facilitate the electronic procurement process for the Canadian Forces. Role Specification Certificates (RSCs) would contain the privileges associated with a particular role while the Role Assignment Certificate (RAC) would assign individuals to a particular role. This design enables roles to be altered without affecting the assignment of roles. [Jan] proposes the use of attribute certificates as a form of passport that would enable mobile agents to execute code on a given system based on the contents of the attribute certificate.

Unfortunately, while attribute certificates are an interesting manner in which to convey privilege they suffer from a number of limitations [Gra01, Wil00] that could prove ultimately detrimental to their eventual widespread adoption. These limitations include the following:

- **Complexity** – Deploying a PKI is a complex undertaking. It is this complexity that has significantly delayed the proliferation of PKI. Had there been a viable alternative to PKI this complexity would have likely derailed it completely. Attribute certificate-based PMI have much of the same complexity (lack of knowledgeable staff, legacy systems, steep learning curve, immature technology, etc.). However, in the case of attribute certificate-based PMI there is not the same hype surrounding the technology and there are viable alternatives.

- **Dependency** – Attribute certificates are cryptographically protected from alteration through the use of a digital signature. This inherent protection is highly beneficial in that it allows attribute certificates to be posted to a public directory or transmitted over a network without fear of modification. Unfortunately, it also creates an extremely restrictive dependency that limits the deployment of this technology to those few environments with an established PKI. The alternative is for organizations to attempt to deploy the two technologies in quick succession, thereby drastically increasing the complexity of the deployment.

P518081.PDF [Page: 17 of 27]

- **Interoperability** – As interoperability testing of PKI products from different vendors has shown, compliance to standards is no guarantee of interoperability between products. In the case of attribute certificates the situation is exacerbated by the use of attribute certificate extensions. These extensions can either be flagged critical or non-critical. Attribute certificates will be rejected if critical extensions aren't recognized.

- **Performance** – As mentioned previously, attribute certificates are cryptographically tied to a PKI. Verification of an attribute certificate involves validating the corresponding digital signature, which in turn requires the verification of at least one public key certificate. In the case of a large attribute certificate-based PMI, privilege will be delegated a number of levels. Validating these delegation paths places significant performance demands on an organization's systems. This performance degradation is only likely to be fully appreciated when an attribute certificate-based PMI has been widely deployed throughout a sizeable organization. When one considers the implications of using this technology in an open environment the performance implications are staggering.

Attribute certificates are without a doubt an intriguing manner in which to convey privilege. However, given the issues mentioned above and the relatively immature state of the technology, it would be foolhardy to contemplate implementing an entirely attribute certificate-based PMI at this time. In time, with a concerted effort amongst authorization technology vendors, attribute certificates may achieve the maturity and interoperability required for widespread deployment. In the current fragmented environment this is a long term prospect. For the present attribute certificates must remain only part of the solution as opposed to the entire solution.

4.3 Standard PMI

There does not currently exist any large-scale implementations of PMI's which have utilized public key or attribute certificates. The technology has so far proven poorly suited or not mature enough for wide-spread implementation. However a review [Mag01] of commercial PMI offerings provides us with a valid general concept of a standard PMI. *It would be an enterprise-wide authorization management system capable of providing controlled access by communities of users to diverse information resources located on disparate computer systems according to a unified security policy. It would also be centrally managed with delegated, de-centralized administration.* This conceptual PMI will be referred to as a standard PMI. Figure 1 is a high-level illustration of such an infrastructure.

In most environments the existing access control capabilities provided by applications and systems are sufficient. What is missing is the capability to configure these distributed access control mechanisms from a central location according to an organization-wide security policy. A standard PMI could conceivably provide this functionality through the use of distributed Access Management Agents. These Agents, co-located with the various systems and applications throughout the organization, would communicate with a central Policy Server in order to promulgate the users, groups and entitlements defined centrally. Access Management Agents have limited functionality as they merely configure distributed access control mechanisms rather than enhance them. Adding or removing all of a user's entitlements to each and every system in an organization is easily accomplished as they are defined and controlled centrally. Furthermore, Access Management Agents can be setup to reconcile the differences between what has been defined centrally and what exists at the system in question. Unauthorized privileges, dormant accounts, etc. can all be automatically deleted, thereby improving the overall security posture of the organization.

P518081.PDF [Page: 18 of 27]

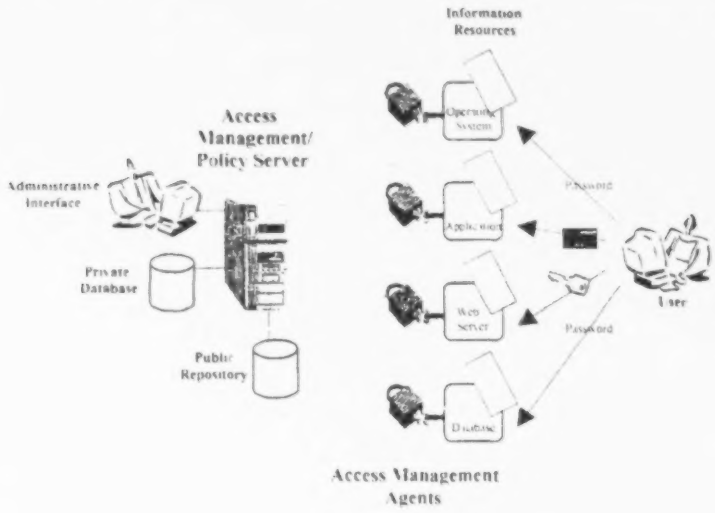

Figure 1 – Standard PMI

While this concept of a standard PMI is innovative and highly suitable, issues arise regarding its use in the classified defence environment Specifically, there are three issues with respect to this design that must be addressed They are as follows

- **Enhanced Access Control** – The standard PMI defines the security policy centrally but relies on the existing access control capabilities of the systems and applications to enforce it For example, a user attempting to access a file on a system running the Solaris operating system would be permitted or denied access based on the native Solaris access control capabilities However, the access control lists governing such access would have been established based on a centrally defined access policy In a classified defence environment the native access control capabilities of the systems and applications are likely to be incapable of providing the enhanced access control required for Multi-Caveat Separation and Multi-Level Security mode of operation

- **Strong Authentication** – The vast majority of systems and applications do not support PKI-based authentication using hardware tokens and biometrics Since access control is entirely dependent on the strength of the authentication mechanism used, a PMI capable of operating in a classified defence environment must address this limitation

- **Sensitivity Labeling** – In a classified defence environment the dissemination of information resources is carefully controlled based on the sensitivity of the information The PMI must be able to label classified information in a trusted manner so that it can be handled accordingly (refer to Note Clearances, Classifications & Caveats)

5.0 Enhanced PMI Proposal

An enhanced PMI consisting of Access Rights Management, Electronic Sensitivity Labeling and Policy-Enforced Access Control (figure 2 is a high-level illustration of such an infrastructure) would address each of these identified deficiencies and be fully capable of managing access in a classified defence environment. Each of these components will be examined in some detail This

P5180861.PDF [Page: 19 of 27]

section will also touch on areas of integration between a PKI and the enhanced PMI to further harden these two technologies

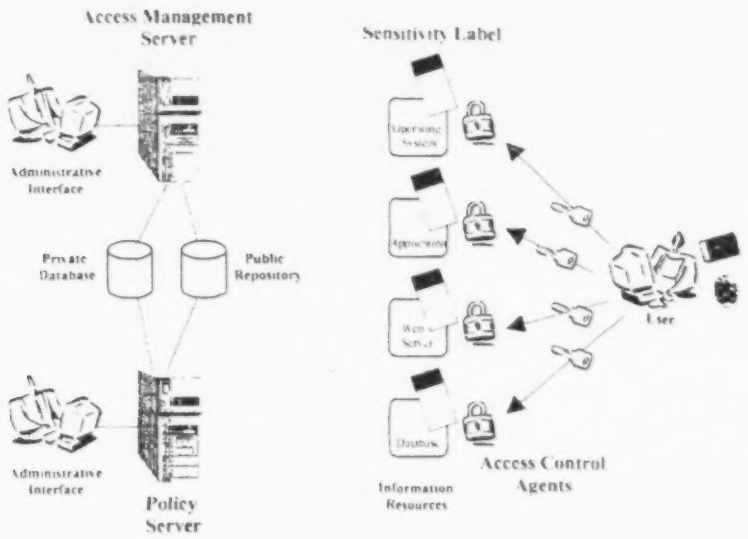

Figure 2 – Enhanced PMI

5.1 Access Rights Management

Security clearance, nationality, rank, military occupation (MOC), role, etc will likely all be determining factors in whether or not an individual should have access to a classified information resource Access Rights Management creates an identity with the corresponding entitlements and then populates this information in a consolidated data store (either a private database or a public directory) Here it is leveraged by the Policy-Enforced Access Control component in determining whether or not access should be provided to a particular information resource Specifically, Access Rights Management is characterized by the following features

- **Role-Based Access Control** - Managing individual user entitlements is a laborious and costly process A better option is to assemble users performing similar functions or with identical attributes into groups or roles and manage their corresponding entitlements en masse This is referred to as Role-Based Access Control (RBAC) For example, the group TOP SECRET might be created to include all military personnel with a TOP SECRET security clearance Likewise, a CELE group might be created to include all Communications and Electronics (CELE) officers

- **Delegated Administration** - It is not realistic to expect a single individual or group to administer all military personnel in a classified defence environment. Apart from the fact that it is a daunting task, it would also be a direct violation of a basic security premise. "Separation of duties" requires that sensitive functions be divided amongst multiple personnel so that no one individual can compromise the system. Delegated administration solves this problem by delegating the management of users and groups to a variety of individuals throughout the organization This has the benefit of providing separation of duties while at the same time giving control to the appropriate authority For example, the administration of the SECRET and TOP SECRET security clearance groups might be tasked to the Special Investigation Unit (SIU) of the military police Likewise, the CELE career manager might be responsible for administering the CELE military occupation group If access to resources is based on the

P518081.PDF [Page: 20 of 27]

aggregate of group and role memberships, then no one individual would be able to compromise the system

- **Rights Enablement Automation** - When a new user is added to the system they will need to be assigned to their respective groups and roles in order to be able to access the information resources required to accomplish their job Likewise, when a user changes jobs or leaves the defence environment entirely they will need to be removed from the respective groups and roles While access can be, and likely will be, terminated immediately by revoking the departing individual's public key credentials, it is prudent to maintain access rights as accurately as possible Since the administration of the various groups and roles may have been distributed throughout the organization, carrying out these processes is no easy task. Rights Enablement Automation facilitates these processes by providing a workflow capability that would automatically contact the appropriate authorities for the necessary approval For example, if a new user were to be added to the classified domain, rights enablement automation could conceivably be configured to send requests to the SIU, the Canadian NATO and the Signals Intelligence (SIGINT) administrators to add this particular user to their respective groups By corroborating this request with their own information the administrator would decide whether or not to approve the request Provided that the requests were approved, the user would have the appropriate entitlements required for him to access the SECRET NATO signals intelligence information resources required to fulfill his job

5.2 Electronic Sensitivity Labeling

As discussed in the note on Clearances, Classifications & Caveats, information resources in a defence environment are classified according to the sensitivity of the information and the potential consequences of this information being compromised For paper-based information resources this marking appears at the top of the page and it is up to individuals to handle the material accordingly NATO, in order to facilitate the secure transmission of electronic information resources between member countries, has been working on developing the digital equivalent of this sensitivity labeling In such an environment the marking *is a piece of electronic data that has been encoded to represent the same sensitivities as in the paper environment* [Inf01] *Attaching a label to electronic information promotes originator awareness of the requirement for correct and consistent marking, facilitates automated access and release control, enables the use of multi-level security systems, and removes the need to thoroughly examine electronic information in order to determine its sensitivity.*[Lab01]

An electronic sensitivity label must be bound [Inf01] to the information resource in such a way that it cannot be removed or altered by unauthorized personnel. In fact, the binding between the marking and the information resource must be every bit as strong as the security provided by other components of the PMI The reason is that an intruder will always attempt to circumvent or attack the weakest link in any security system If the binding were the weakest link the intruder would merely change the classification or the release control in order to provide themselves access to the classified resource. Two alternatives [Lab01] capable of providing this binding are as follows

- **Security Server** – The Security Server would store electronic sensitivity labels for each information resource in such a way that when the information resource is accessed the corresponding label would automatically be processed as well

- **Digital Signature** – A digital signature would be used to tie the electronic sensitivity label to the information resource Any modification of either the information resource or the label would invalidate the binding linking them

P518081.PDF [Page: 21 of 27]

While Electronic Sensitivity Labeling is a critical component in implementing a PMI in a defence environment, the specifics for such an implementation are outside of the scope of this paper Those wishing to undertake such a task would be well-advised to reference the work in this area being undertaken on behalf of NATO in order to not only leverage the accumulated expertise but to ensure compliance with future directives

5.3 Policy-Enforced Access Control

The Access Rights Management component populated a common data store with user identity, group/role and entitlements information The Electronic Sensitivity Labeling component appropriately marked classified information resources by securely binding a sensitivity label to them It is left to the Policy-Enforced Access Control component the task of deciding whether or not a particular user can access a given information resource This process consists of an access control enforcement function and an access control decision function The access control enforcement function permits access to information resources only when the access has been approved by the access control decision function

In an enhanced PMI distributed Access Control Agents assume the role of access control enforcement function When an authenticated user attempts to access a protected information resource it is the Access Control Agent which blocks the access attempt Meanwhile, it sends the identity of the user and the sensitivity label of the resource to the Policy Server The Policy Server, having evaluated the access request in light of the security policies in place, will send back an access approved or access denied message The Access Control Agent will in turn enforce this decision In the case of an access approved message it will allow the access to the information resource to proceed unimpeded In the case of an access denied message it will block the access attempt and display the appropriate message to the user Whereas Access Management Agents in a standard PMI rely on the native access control capability of the system or application and are therefore quite simple, Access Control Agents in an enhanced PMI supplement the native access control capability of the system or application As a result, they are quite complex in nature These Access Control Agents can even be used to support strong authentication to the system or application using public key credentials This is discussed in further detail in section 5 4 entitled PKI Integration

The Policy Server assumes the role of access control decision function. In actuality it does more than just mediate the access requests however It performs the following functions

- **Control** – Policy-Enforced Access Control enables an organization to define security policies centrally while enforcing them consistently throughout the organization The security policy or rules defined centrally can be as simple or complex as required Complex policies can make access decisions based on dynamic information, take behavioral patterns into consideration and even react to access attempts in various ways. It is critical that the security policy governing access to a particular information resource can't be circumvented merely by copying the resource to a new system The security policy must migrate with the resource so that it is consistently protected regardless of where it is located within the organization

- **Monitor** – Policy-enforced access control allows an organization to appropriately monitor information access This information is maintained in a protected audit log. The system can even be setup to audit access attempts but not actually enforce the security policy In the audit log of the various transactions it would indicate whether access would have been allowed had the policy been enforced This capability allows an organization to effectively test their security policies prior to actually enforcing them

- **React** – Policy-enforced access control allows security policies and access violation policies that react to access attempts to be established For example, if a particular information

P515081.PDF [Page: 22 of 27]

resource is accessed, either successfully or unsuccessfully, an e-mail notifying the owner of the resource can be sent automatically

5.4 PKI Integration

A PKI with the appropriate level of private key protection and an enhanced PMI are both well suited to managing identity and access in a classified defence environment. However, by integrating the two technologies efficiencies can be gained and the overall security of both technologies improved. This section touches on a number of these potential areas of integration.

Access Rights Management

- **Administration** - Creating users and groups within a PKI and then having to do the same for a PMI is a redundant process. Significant savings can be achieved by synchronizing these processes through a single administrative effort. In a number of COTS products there exists this common interface or an Access Management Agent capable of adding a user to a PKI once they have been created in the PMI. Consolidating the administration function for these two infrastructures is not always desirable. Within many organizations the personnel responsible for these functions are not necessarily the same. Furthermore, unless properly handled it can increase the likelihood of a security compromise by placing too much power in any one group's hands ("separation of duty").

- **Rights Enablement Automation** – Rights Enablement Automation is potentially a key area of integration. The digital signature infrastructure provided by the PKI can be leveraged to provide enhanced security and non-repudiation for the Access Rights Management workflow capability. Requests for additional entitlements and role/group membership can be digitally signed by human resources or the user himself. These requests would then be automatically forwarded to the appropriate authorities who would in turn digitally sign the request. Provided that the digital signatures were valid the user would receive the requested entitlements.

Electronic Sensitivity Labeling

- **Binding** – Digital signatures are one of the two methods outlined for providing the binding between the sensitivity label and the information resource. Digital signatures are an attractive option in that they cryptographically bind the two pieces of data together in a manner that facilitates detection of any tampering.

Policy-Enforced Access Control

- **Certificate-based authentication** – In an enhanced PMI, Access Control Agents will be capable of supporting certificate-based authentication of users. Typically, the Access Control Agent extracts the pertinent information out of the certificate and passes it back to the Policy Server to complete the authentication process. This information is likely to consist of the identity of the user but it can be expanded to include information stored in the certificate extensions. An integral component of certificate-based authentication is Certificate Revocation List (CRL) checking. This can include basic CRL checking or advanced CRL checking including support for CRL distribution points and Online Certificate Status Protocol (OCSP).

- **Deployment** - As with any infrastructure product, deploying a PKI is a laborious and time-consuming process that could conceivably take months to years depending on the size of the

P518081.PDF [Page: 23 of 27]

organization An enhanced PMI can facilitate this process by providing support for the gradual deployment of PKI This is accomplished by permitting access to protected information resources through certificate-based and basic authentication (user name and password) When PKI has finally been rolled out to the whole organization this can be changed to permit only certificate-based authentication

- **Component Integration** - Communications between Access Control Agents and the Policy Server need to be secured in terms of confidentiality, integrity and mutual authentication This can best be accomplished by issuing public-key credentials to the Policy Server along with each Agent This requires either an enterprise-wide PKI or PKI functionality built into the PMI An additional benefit to this approach is the capability to instantaneously revoke a compromised agent

General

- **Common Repository** – Non-sensitive or protected (using digital signatures or encryption) access and identity information should be stored in a public repository Likewise, sensitive or unprotected access and identity information should be stored in a private database These common data stores facilitate administration, enhance interoperability and improve auditability of identity and access throughout an organization

6.0 Conclusions

The classified defence environment is an extremely challenging environment due to a reliance on information resources, disparate highly networked information systems, high turnover of personnel and rigorous security requirements In their current incarnations commercial-off-the-shelf Public Key Infrastructure (PKI) and Privilege Management Infrastructure (PMI) products are not sufficient for this environment

The primary weakness in PKI implementations is with respect to private key protection While validated hardware tokens mitigate a number of inherent vulnerabilities in workstation security they are still reliant on PINs or passwords for two-factor authentication In a classified defence environment password authentication needs to be replaced with biometric authentication While biometrics have long been considered unsuitable for most environments, they are well-suited to the classified defence environment with its unique requirements. Utilizing hardware tokens, specifically PC tokens, and biometrics in conjunction with PKI provides the strongest form of authentication on which to base access decisions

Access control capabilities native to most systems and applications are incapable of providing the necessary level of protection required for sensitive information assets An enhanced PMI, consisting of Access Rights Management, Electronic Sensitivity Labeling and Policy-Enforced Access Control components, rectifies a number of deficiencies in the standard PMI model and as a result provides the necessary level of protection to information resources throughout a classified defence environment Implementing an enhanced PMI will require bridging the gap between the requirements of the classified defence environment and the functionality provided by existing COTS PMI products

PKI and PMI are complementary technologies The overall level of security can be significantly improved by integrating the two technologies so as to take advantage of their relative strengths Given the widespread deployment of PKI technology in defence departments throughout the world now is a good time to improve upon the strong authentication available to provide enhanced access control using PMI The implementation of PKI and PMI will enable the classified defence environment to shift from a predominantly network-based information security model,

P518081.PDF [Page: 24 of 27]

operating in System High Mode, to a content-based information security model capable of supporting Multi-Caveat Separation and Multi-Level Security mode of operation. A proof-of-concept study validating this approach needs to be undertaken.

7.0 References

[Cav01] Caveat Separation – Architecture, Concept of Operations and Detailed Design, Department of National Defence, April 12, 2001

[Cha01] The Challenge of User Authentication, Ankari, 2001

[Con01] Consistent Marking of NATO Information Version 2.0, NATO, September 20,2001

[Day01] Roseann Day, John Daly, Charles Kolodgy and Chris Christiansen, "Policy-Based Provisioning Simplifying and Streamlining Access Rights Management", IDC, July 2001

[DMH01] Defence Message Handling System (DMHS) Web Site <URL http //img mil ca/dmhs_pmo/migration_pages/demsII_e htm

[DMS01] Defense Message System Public Access Web Site <URL http //www.disa mil/D2/dms/>

[DTS01] Defense Travel System Program Management Office <URL http //www dtic mil/travelink/>

[Ele01] Electronic Authorization Study – Business Requirements Report, Communications Security Establishment, May 9, 2001

[Ell00] Carl Ellison and Bruce Schneier, " Ten Risks of PKI What You're not Being Told about Public Key Infrastructure," Computer Security Journal, v 16, n 1, 2000, pp 1-7

[Fra01] Scott Frazee, "Biometrics Why Bother?", SANS Institute, June 29, 2001

[Gra01] Christopher Grandy, "Using a Privilege Management Infrastructure to Support Business Processes Within the Department of National Defence and the Canadian Forces", Royal Military College, April 2001.

[Her01] Colleen M Herrmann, "Common Access Card (CAC), Security, and Privacy", <URL http //www.chips navy mil/archives/01_summer/cac htm>

[Inf01] Infosec Technical Directive for Labeling of NATO Information in Electronic Format Version 2.0, NATO, September 20, 2001

[Jan] Wayne Jansen and Tom Karygiannis, "Privilege Management of Mobile Agents," National Institute of Standards and Technology

[Lab01] Electronic Labeling of NATO Information Version 2.0, NATO, September 20, 2001

[Mag99] Alan Magar, "The Role of Public Key Infrastructure and Privilege Management Infrastructure in Defensive Information Warfare", University of London, September 1, 1999

[Mag01] Alan Magar, "Privilege Management Infrastructure", Defence Research Establishment Ottawa, March 30, 2001

[Wil00] Stephen Wilson, "Some Limitations of Attribute Certificates", beTRUSTed, Cryptographic Centre of Excellence (CCE) Journal, Issue 3, 2000

P518081.PDF [Page: 25 of 27]

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1 ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Magar Security Architecture Inc
160 Gladstone Avenue,
OTTAWA K2P 0Y3

2 SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3 TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

Managing Identity and Access in a Classified Defence Environment (U)

4 AUTHORS (Last name, first name, middle initial)

Magar, Alan

5 DATE OF PUBLICATION (month and year of publication of document)	6a NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)	6b NO. OF REFS (total cited in document)
October, 2001	21	18

7 DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report (Final)

8 SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

Defence Research Establishment Ottawa/Information Operations Section
101 Colonel By Drive
OTTAWA K1A 0Z4

9a PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)	9b CONTRACT NO. (if appropriate, the applicable number under which the document was written)
5BF27	W7714-1-0492

10a ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)
DREO-2001-02	CR-2001-081

11 DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

- (x) Unlimited distribution
- ( ) Distribution limited to defence departments and defence contractors, further distribution only as approved
- ( ) Distribution limited to defence departments and Canadian defence contractors, further distribution only as approved
- ( ) Distribution limited to government departments and agencies, further distribution only as approved
- ( ) Distribution limited to defence departments, further distribution only as approved
- ( ) Other (please specify)

12 DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

Full Unlimited

13 ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual)

(U) The classified defence environment is an extremely challenging environment where the rigorous protection of information assets has necessitated the adoption of a predominantly network-based information security model operating in System High Mode. Two innovative technologies, Public Key Infrastructure and Privilege Management Infrastructure, provide the underlying infrastructure with which to manage identity and access throughout an organization. This paper will examine how these two technologies can be enhanced in order to transition the classified defence environment to a content-based information security model capable of providing Multi-Caveat Separation and eventually supporting, Multi-Level Security mode.

14 KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Access Control
Attribute Certificates
Authentication
Authorization
Caveat Separation
Identity Management
Multi-Level Security
PKI
PMI
Provisioning
Privilege Management Infrastructure
Public Key Infrastructure

P5180081.PDF [Page: 27 of 27]

Defence R&D Canada
is the national authority for providing
Science and Technology (S&T) leadership
in the advancement and maintenance
of Canada's defence capabilities.

R et D pour la défense Canada
est responsable, au niveau national, pour
les sciences et la technologie (S et T)
au service de l'avancement et du maintien des
capacités de défense du Canada.

#5180081

CA021

DEFENCE R&D DÉFENSE

www.drdc-rddc.dnd.ca